STATE OF ALABAMA

Information Technology Standard

Standard 620-01S1: Access Management

1. INTRODUCTION:

A comprehensive access account management process ensures that only authorized users gain access to workstations, applications, networks, and data, and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.

2. OBJECTIVE:

Manage the granting and rescinding of access to State of Alabama networks and information systems, plan and utilize appropriate access enforcement mechanisms, and ensure user accountability.

3. SCOPE:

These requirements apply to all managers and administrators (State employees, contractors, vendors, and business partners) of any State of Alabama information system resources.

4. REQUIREMENTS:

The following State of Alabama requirements are based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-53: Recommended Security Controls for Federal Information Systems, and other best practices.

4.1 ACCOUNT MANAGEMENT

Policy: Organizations shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

4.1.1 Access Authorization

System and Network Administrators shall:

- Ensure that all requests to establish access accounts are approved by a designated manager, supervisor, or the system owner.
- Maintain a record of all users authorized to access the system identifying the user name and unique user ID, level of authority granted, user location, the date access was granted, and the date access will terminate (or was terminated).
- Monitor and review the granting and rescinding of network and system access.
- Ensure user accounts are reviewed periodically and inactive accounts are removed.

4.1.2 Temporary Access

Temporary access may be granted if required for service providers (contractors, vendors, and business partners) or external regulators.

All requests for temporary access shall be made in writing and shall be subject to management or system owner approval.

Temporary access shall be valid only for a specified period of time and shall be disabled immediately upon expiration or when no longer required, whichever occurs first.

Short-term (less than one day) access to the State network without identification or authentication shall be limited to Internet access and connections to other publicly available information systems. Access points providing unauthenticated access shall be closely monitored and, when practical, shall be disabled if/when not needed.

4.1.3 Access Termination

Managers/Supervisors shall:

- Notify applicable System Administrator(s) in writing within 48 hours of an employee termination, start of long-term (greater than 30 days) leave, or a contract person completing their assignment. If termination is for cause, notification shall be made immediately upon or prior to termination action.
- Advise administrators of actions regarding disposition of user files and email accounts.

Network and System Administrators shall:

- Disable access to networks, application systems, and data when advised by management.
- Network access shall be disabled immediately when a user is terminated for cause.
- User accounts inactive for more than 30 days shall be disabled.
- Unless instructed otherwise, delete inactive or disabled accounts after 60 days inactivity.
- Periodically review user accounts to ensure compliance with this standard.

4.2 ACCESS ENFORCEMENT

Access to all State information is determined by both its protection category and user need-to-know. Need-to-know shall be determined by the information owner and enforced by role-based or discretionary access controls. Access controls shall be established and enforced for all shared or networked file systems and internal websites. All non-public websites shall be organized to provide at least three distinct levels of access:

(1) Open access to general information that is made available to all authorized users with network access. Access does not require an audit transaction.

(2) Controlled access to information that is made available to all authorized users upon the presentation of an individual authenticator. Access shall be recorded in an audit transaction.

(3) Restricted access to need-to-know information that is made available only to an authorized community of interest. Authorized users must present an individual authenticator and have either a demonstrated or validated need-to-know. All access to need-to-know information and all failed access attempts shall be recorded in audit transactions.

4.2.1 Access Enforcement Mechanisms

Access control policies (e.g., identity-based policies, role-based policies, ruled-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in State information systems.

In addition to controlling access at the information system level, access enforcement mechanisms shall be employed at the application level, when necessary, to provide increased information security.

Ensure that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).

4.2.2 Separation of Duties and Least Privilege

Access procedures shall enforce the principles of separation of duties and least privilege.

Information systems shall enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions.

4.3 SUPERVISION AND REVIEW

Policy: Users are hereby advised that authorized access does not imply a right to privacy. System and network activities may be monitored, recorded, and are subject to audit by management or other authorized personnel.

Management or authorized personnel shall review audit records (e.g., user activity logs) for inappropriate activities in accordance with State policies and standards. Investigate any unusual information system-related activities and periodically review changes to access authorizations.

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 620-01: Network and Systems Access
http://isd.alabama.gov/policy/Policy_620-01_Network_System_Access.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	1/12/2007	Replaces Policy 620-02: Access Termination